REMARKS

Claims 1-15 and 18-23 are pending. Claims 1, 6, 7, 12, 14, 18, and 21-23 are amended. Claims 16 and 17 are canceled. Applicants respectfully request reconsideration of the claims in view of the following remarks.

I. Telephone Interview

Applicants' representative contacted the Examiner to conduct a telephone interview prior to the response due date of the Office Action. However, due to the Examiner's schedule, a telephone interview was not able to be scheduled prior to the response due date. Therefore, Applicants respectfully request that the Examiner contact Applicants' representative to discuss this application prior to taking any further action on this case.

II. Claim Objections

The Office objects to claim 21 because of minor informalities. Applicants amend claim 21 to change "system" to "method," as suggested in the Office Action. Therefore, Applicants respectfully request withdrawal of the objection to claim 21.

III. 35 U.S.C. § 101, Allegedly Non-Statutory Subject Matter in Claims 1-23

The Office rejects claims 1-23 under 35 U.S.C. § 101 as allegedly being drawn to non-statutory subject matter. With respect to claims 1-11, 16-17, and 22-23, the Office Action states that the Examiner interprets these claims as being software *per se*.

With respect to claims 1-11, the Office Action states that the elements of the system "are all taken to be, by the examiner, intrinsically as being software configured to perform an action but failing to provide a tangible result." It is unclear whether the Examiner is interpreting the elements as software *per se* or as software configured to perform an action. Software *per se* cannot perform any action. Software must be executed on some device or structurally tied to some computer readable medium to realize its function. For an example of a system embodiment, the specification states:

> It is further noted that, unless indicated otherwise, all functions described herein may be performed in either hardware or software, or in some combinations thereof. In a preferred embodiment, however, the functions are performed by a processor such as a computer or an electronic data processor in accordance with code such as computer program code, software, and/or integrated circuits that are coded to perform such functions, unless indicated otherwise.

Specification, page 3, lines 8-15. Clearly, a random value generator, for example, cannot be disembodied computer code, because computer code without a device on which to execute cannot generate anything. Therefore, the system of claim 1, for instance, must be either hardware or a combination of hardware and software, as supported by the specification. More particularly, the system of claim 1 may be specific hardware, software running on a processor, or a combination of specific hardware and software running on a processor.

With respect to providing a tangible result, Applicants amend independent claim 1 to recite transmitting a secure message to a message target. Transmission of a secure message from a message source to a message target provides a concrete, useful, and tangible result. Applicants amend independent claim 7 to recite receiving a secure message transmitted from a message source and unmasking the secure message at the message target. Receipt of a secure message and unmasking the secure message provide a concrete, useful, and tangible result.

With respect to claims 12-15 and 18-21, the Office Action states that the claims fail to produce a tangible result. Applicants amend independent claims 12 and 18 in a manner similar to claims 1 and 7, respectively; therefore, claims 12 and 18 are statutory for at least the same reasons.

With respect to claims 22 and 23, the Office Action states that claims 22 and 23 are software *per se* and fail to provide a tangible result. The Examiner alleges that the claims lack a "proper" computer readable medium. Applicants amend independent claims 22 and 23 in a manner similar to claims 1 and 7, respectively; therefore, claims 22 and 23 are statutory for at least the same reasons. Furthermore, Applicants amend claims 22 and 23 to recite a computer readable medium.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 1-15 and 18-23 under 35 U.S.C. § 101.

IV. 35 U.S.C. § 102, Alleged Anticipation of Claims 1-23

The Office rejects claims 1-23 under 35 U.S.C. § 102(e) as allegedly being anticipated by *Shrader* et al. (U.S. Patent No. 6,914,985). Applicants respectfully traverse this rejection.

Shrader discloses a method and system for presentation and manipulation of public key cryptography standard (PKCS) enveloped data objects. *Shrader* teaches a data processing system may create, modify, transmit, store, and receive cryptographic data objects formatted according to interoperably defined cryptography standards, such as PKCS #7 EnvelopedData objects. See *Shrader*, col. 6, lines 63-67. *Shrader* generally teaches about digital certificates, public keys, private keys, hash functions, and the like. More particularly, *Shrader* teaches that enveloped data is constructed as follows:

> Enveloped-data is constructed by the following steps:
> 1. A content-encryption key for a particular content-encryption algorithm is generated at random.
> 2. The content-encryption key is encrypted for each recipient. The details of this encryption depend on the key management algorithm used, but three general techniques are supported:
>   key transport: the content-encryption key is encrypted in the recipient's public key;
>   key agreement: the recipient's public key and the sender's private key are used to generate a pairwise symmetric key, then the content-encryption key is encrypted in the pairwise symmetric key; and
>   symmetric key-encryption keys: the content-encryption key is encrypted in a previously distributed symmetric key-encryption key.
> 3. For each recipient, the encrypted content-encryption key and other recipient-specific information are collected into a RecipientInfo value.
> 4. The content is encrypted with the content-encryption key. Content encryption may require that the content be padded to a multiple of some block size.
> 5. The RecipientInfo values for all the recipients are collected together with the encrypted content to form an EnvelopedData value.
>
> A recipient opens the digital envelope by decrypting one of the encrypted content-encryption keys and then decrypting the encrypted content with the recovered content-encryption key.

Shrader, col. 11, line 45, to col. 12, line 7. Thus, *Shrader* teaches generating an enveloped data object by providing a content-encryption key for each recipient, encrypting the content-encryption key for each recipient, collecting the encrypted content-encryption key and other recipient-specific information into a RecipientInfo value, encrypting the content with the content-encryption key, and collecting the RecipientInfo values for all the recipients with the encrypted content to form an EnvelopedData value.

In contradistinction, with respect to claim 1, for example, the present invention provides a system comprising a random value generator configured to generate a random value. A message validation code generator coupled to the random value generator is configured to generate a message validation code based on a predetermined key, a message, and the random value. A one-time pad generator coupled to the random number generator is configured to generate a one-time pad based on the random value and the predetermined key. A masked message generator coupled to the one-time pad generator is configured to generate a masked message based on the one-time pad and the message. A transmitter is configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target. The message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

With respect to claim 1, the Office Action alleges that *Shrader* teaches a message validation code because *Shrader* states that the enveloped data have validation checks. The cited portions of *Shrader* are as follows:

> PKCS #7 describes a general syntax for data that may have cryptography applied to it. In other words, PKCS #7 defines the syntax for several cryptographically protected messages, including encrypted messages and messages with digital signatures. The syntax admits recursion, so that one envelope can be nested inside another or one party can sign previously enveloped digital data. PKCS #7 also allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and it also provides for other attributes, such as countersignatures, to be associated with a signature.

Shrader, col. 2, lines 19-29.

> Existing EnvelopedData objects could be dragged and dropped onto the interface to view a preconstructed EnvelopedData object. The interface could also export a EnvelopedData object that passes validation to a file or other transfer mechanism, such as the clipboard, in a DER-encoded format. Before the EnvelopedData object is exported or stored, the interface will run the defined elements through a set of verification rules, presenting errors to the user if present. The same validation checks will also occur when a EnvelopedData object is imported into the interface.

Shrader, col. 13, lines 57-67. Thus, *Shrader* appears to teach attributes to be authenticated and an enveloped data object that passes validation to a file or other transfer mechanism. However, the Office Action proffers no explanation as to how this somehow anticipates a message validation **code generator** that is configured to generate a message validation code that is transmitted to the message target and used by the message target to validate the message.

The Office Action alleges that *Shrader* teaches that the message validation code is based on a predetermined key because *Shrader* states how the Public-key cryptography standard is applied within the invention. The cited portions of *Shrader* are as follows:

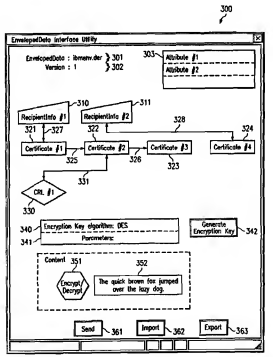

FIG. 3

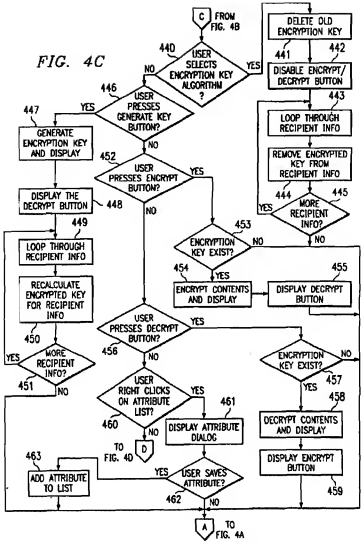
C
FROM FIG. 4B
USER SELECTS ENCRYPTION KEY ALGORITHM ?
440
NO
YES
USER PRESSES GENERATE KEY BUTTON?
446
YES
NO
GENERATE ENCRYPTION KEY AND DISPLAY
447
USER PRESSES ENCRYPT BUTTON?
452
YES
NO
DISPLAY THE DECRYPT BUTTON
448
LOOP THROUGH RECIPIENT INFO
449
RECALCULATE ENCRYPTED KEY FOR RECIPIENT INFO
450
MORE RECIPIENT INFO?
451
YES
NO
USER PRESSES DECRYPT BUTTON?
456
YES
NO
USER RIGHT CLICKS ON ATTRIBUTE LIST?
460
YES
NO
DISPLAY ATTRIBUTE DIALOG
461
TO FIG. 40
D
ADD ATTRIBUTE TO LIST
463
USER SAVES ATTRIBUTE?
462
YES
NO
A
TO FIG. 4A
DELETE OLD ENCRYPTION KEY
441
442
DISABLE ENCRYPT/ DECRYPT BUTTON
443
LOOP THROUGH RECIPIENT INFO
REMOVE ENCRYPTED KEY FROM RECIPIENT INFO
444
445
MORE RECIPIENT INFO?
YES
NO
453
ENCRYPTION KEY EXIST?
NO
YES
454
455
ENCRYPT CONTENTS AND DISPLAY
DISPLAY DECRYPT BUTTON
ENCRYPTION KEY EXIST?
NO
YES
457
458
DECRYPT CONTENTS AND DISPLAY
DISPLAY ENCRYPT BUTTON
459

FIG. 4C

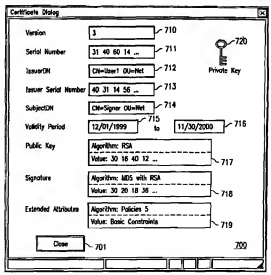
Certificate Dialog
Version
3
710
Serial Number
31 40 60 14 ...
711
720
IssuerDN
CN=Issuer1 OU=Net
712
Private Key
Issuer Serial Number
40 31 14 56 ...
713
SubjectDN
CN=Signer OU=Net
714
Validity Period
12/01/1999
715
to
11/30/2000
716
Public Key
Algorithm: RSA
Value: 30 16 40 12 ...
717
Signature
Algorithm: MD5 with RSA
Value: 30 20 18 36 ...
718
Extended Attributes
Algorithm: Policies 5
Value: Basic Constraints
719
Close
701
700

FIG. 7

> Public-key cryptography is the technology in which encryption and decryption involve different keys. The two keys are the public key and the private key, and either can encrypt or decrypt data. A user gives his or her public key to other users, keeping the private key to himself or herself. Data encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.
>
> As public-key cryptography has gained acceptance, standards have become necessary so that software at two different sites could work together even when the software is developed by different vendors. In particular, standards have been developed to allow agreement on digital signatures, digital enveloping, digital certification, and key agreement. However, interoperability requires strict adherence to communicable formats, and PKCS, or "Public Key Cryptography Standard," provides a basis for interoperable standards in heterogeneous environments.

Shrader, col. 1, lines 27-43. None of the cited portions teaches or suggests a message validation code generator that generates a message validation code based on a predetermined key, a message, and a random number, as recited in claim 1, for example.

Any reference disclosing cryptographic techniques is likely to include words such as "authentication," "key," "hash," and "random" here and there throughout the reference. However, it is the burden of the Office to establish a *prima facie* case of anticipation for the claims, not merely to point to where certain words appear. That is, the Office must address the claim as a whole, demonstrating that the reference teaches each and every claim feature, arranged as they are in the claims. Here, the Office Action appears to cite seemingly arbitrary, albeit lengthy, portions of *Shrader* as allegedly teaching bits and pieces of the claim without explaining how those pieces supposedly fit together to form the present invention.

As a further example, the Office Action alleges that *Shrader* teaches a one-time pad generator that is configured to generate a one-time pad based on the random value and the predetermined key and a masked message generator that is configured to generate a masked message based on the one-time pad, because *Shrader* appears to teach padding encrypted content to a multiple of some block size. However, the Office Action does not explain how padding already encrypted content is somehow equivalent to generating a one-time pad based on a key **and then** masking the message. A person of ordinary skill

in the art would not find the teaching of *Shrader* to be equivalent to the invention recited in claim 1, for instance.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

Applicants submit the Office does not establish a *prima facie* case of anticipation for claim 1. Independent claims 12 and 22 recite features addressed above with respect to claim 1 and are allowable for similar reasons. Since claims 2-6 and 13-15 depend from claims 1 and 12, the same distinctions between *Shrader* and the invention recited in claims 1 and 12 apply for these claims. In addition, claims 2-6 and 13-15 recite further combinations of features not taught by *Shrader*.

With respect to claims 2-6 and 13-15, the Office Action seems to cite more arbitrary portions of the reference simply because the reference uses similar terms. However, Applicants submit that the Office Action does not provide enough explanation as to why the teachings of *Shrader* somehow anticipate the claims. In other words, the Office does not establish a *prima facie* case of anticipation for claims 2-6 and 13-15.

More particularly, with respect to claim 5, for example, the Office Action alleges that *Shrader* teaches a protected message envelope generator that generates a protected message envelope based on the random value, the message validation code, and the masked message, because various portions of the reference allegedly teach a content-encryption key being encrypted at random, attributes to be authenticated, and an encryption messaging process. The Office Action fails to address the claim as a whole. *Shrader* appears to teach pieces of the claimed invention, because *Shrader* is in the same field of endeavor and uses similar terms. However, *Shrader* does not teach the claim features **arranged as they are in the claims**. That is, *Shrader* does not teach generating a random value and generating a message validation code based on the random value, a

predetermined key, and a message (*Shrader* actually teaches generating a key randomly, not a predetermined key **plus** a random value); *Shrader* does not teach generating a one-time pad **based on the random value and the predetermined key**; *Shrader* does not teach generating a masked message **based on the one-time pad and the predetermined key**; and, *Shrader* does not teach generating a protected message envelope **based on the random value, the message validation code, and the masked message**. Clearly, *Shrader* does not anticipate claim 5, because *Shrader* does not teach each and every claim feature.

With respect to claim 7, the Office Action alleges that *Shrader* teaches a protected message envelope reader that extracts a random value generated at the message source, a masked message, and a message validation code from a received protected message envelope, and cites seemingly arbitrary portions of *Shrader* without explanation of how *Shrader* somehow anticipates the combination of features in claim 7. As stated above, *Shrader* appears to teach attributes to be authenticated and an enveloped data object that passes validation to a file or other transfer mechanism. However, the Office Action proffers no explanation as to how this somehow anticipates a message validation **code** that is used by the message target to validate the message. Furthermore, the Office Action does not address how *Shrader* somehow teaches extracting from the enveloped data object a random value that was generated at the message source.

Applicants submit the Office does not establish a *prima facie* case of anticipation for claim 7. Independent claims 18 and 23 recite features addressed above with respect to claim 7 and are allowable for similar reasons. Since claims 8-11 and 19-21 depend from claims 7 and 18, the same distinctions between *Shrader* and the invention recited in claims 7 and 18 apply for these claims. In addition, claims 8-11 and 19-21 recite further combinations of features not taught by *Shrader*.

With respect to claims 8-11 and 19-21, the Office Action seems to cite more arbitrary portions of the reference simply because the reference uses similar terms. However, Applicants submit that the Office Action does not provide enough explanation as to why the teachings of *Shrader* somehow anticipate the claims. In other words, the Office does not establish a *prima facie* case of anticipation for claims 8-11 and 19-21.

More particularly, with respect to claim 9, the Office Action alleges that *Shrader* teaches a message validation code comparator that compares a received message validation code with a generated message validation code, because *Shrader* mentions a form of the word "authenticate." Applicants respectfully disagree. Merely mentioning a form of the word "authenticate" is not nearly enough to anticipate the combination of features recited in claim 7, because *Shrader* does not teach a message validation code generator at the message target, a protected message envelope reader that extracts a message validation code from the protected message envelope received from the message source, and a message validation code comparator that compares the message validation code generated at the message target with the message validation code received from the message source. Again, the Office simply fails to establish a *prima facie* case of anticipation for claim 9, for example.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 1-15 and 18-23 under 35 U.S.C. § 102(e).

V. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: 5/3/2007

Stephen R. Tkacs
Reg. No. 46,430
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6422
AGENT FOR APPLICANTS